SF-058/PCT

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平8－125651

(43)公開日　平成８年(1996)５月17日

(51)Int.Cl.[6]		識別記号	庁内整理番号	Ｆ Ｉ	技術表示箇所
Ｈ０４Ｌ	9/00				
	9/10				
	9/12				
Ｇ０９Ｃ	1/00		7259－5Ｊ		
				Ｈ０４Ｌ　9/00　Ｚ	

審査請求　未請求　請求項の数８　ＯＬ　（全 16 頁）　最終頁に続く

(21)出願番号　特願平6－264881

(22)出願日　平成６年(1994)10月28日

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地

(72)発明者　早川　弘之
神奈川県横浜市戸塚区吉田町292番地　株式会社日立製作所情報映像メディア事業部内

(72)発明者　▲吉▼澤　和彦
神奈川県横浜市戸塚区吉田町292番地　株式会社日立製作所映像メディア研究所内

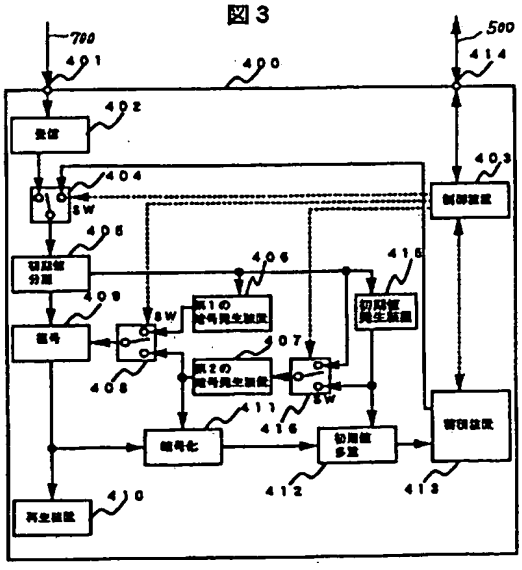
(74)代理人　弁理士　高田　幸彦

最終頁に続く

(54)【発明の名称】　信号処理装置

(57)【要約】
【目的】暗号化された放送データの著作権を保護しつつ該データ信号の蓄積，伝送を可能とする。
【構成】通信衛星から受信した暗号化された放送データ信号を復号装置４０９で復号し、再生装置４１０で再生する。復号信号は、暗号化装置４１１で再暗号化して蓄積装置４１３に蓄積し、あるいは装置外部に伝送する。復号した放送データの蓄積及び伝送は該データを再暗号化して行なうので、複製による不正な使用が困難であり、データの著作権を保護しつつ蓄積装置に蓄積して利用することができる。

図３



1

【特許請求の範囲】

【請求項１】暗号化された入力信号の中から暗号の初期値を抽出する初期値抽出手段と、前記初期値をもとに第１の暗号を発生させる第１の暗号発生手段と、前記暗号化された入力信号を前記第１の暗号を使用して復号する復号手段とを備えた信号処理装置において、

前記初期値抽出手段で抽出した初期値をもとにして新たな初期値を発生させる初期値発生手段と、

前記初期値発生手段で発生させた新たな初期値をもとにして第２の暗号を発生させる第２の暗号発生手段と、

前記第２の暗号発生手段で発生させた第２の暗号を用いて前記復号した入力信号を再暗号化する再暗号化手段と、

前記再暗号化手段で再暗号化した信号に前記新たな初期値を多重化して出力する暗号の初期値多重化手段とを設けたことを特徴とする信号処理装置。

【請求項２】請求項１において、前記初期値発生手段は、暗号化された入力信号の中から抽出した暗号の初期値をそのまま出力することを特徴とする信号処理装置。

【請求項３】請求項１において、前記第２の暗号発生手段の一部または全体、及び／または前記暗号化手段の一部または全体を着脱可能としたことを特徴とする信号処理装置。

【請求項４】暗号化された入力信号の中から暗号の初期値を抽出し、前記初期値をもとに暗号を発生させ、前記暗号化された入力信号を前記暗号を使用して復号して出力するようにした信号処理装置において、

複数の暗号化信号を入力する暗号化信号入力手段と、

前記暗号化信号入力手段で入力した複数の暗号化信号の何れかを選択して出力する暗号化信号の入力選択手段と、

前記選択された暗号化信号の中から暗号の初期値を抽出する初期値抽出手段と、　前記初期値抽出手段により抽出された初期値をもとに複数の暗号を発生させる暗号発生手段と、

前記暗号発生手段からの暗号を選択して出力する暗号選択手段と、

前記暗号選択手段で選択した暗号をもとにして前記入力選択手段で入力した暗号化信号を復号する復号手段とを設けたことを特徴とする信号処理装置。

【請求項５】請求項４において、前記暗号発生手段はその一部または全体が着脱可能な複数の暗号発生手段から成り、または／及び、前記復号化手段の一部または全体を着脱可能としたことを特徴とする信号処理装置。

【請求項６】暗号化された入力信号の中から暗号の初期値を抽出し、前記初期値をもとに暗号を発生させ、前記暗号化された入力信号を前記暗号を使用して復号して出力するようにした信号処理装置において、

２つの暗号化信号入力手段と、

前記２つの暗号化信号入力手段で入力した暗号化信号の

2

何れかを選択して出力する暗号化信号の入力選択手段と、

前記選択された暗号化信号の中から初期値を抽出する初期値抽出手段と、

前記抽出された初期値をもとにして第１の暗号を発生させる第１の暗号発生手段と、

前記抽出された初期値をもとにして新たな初期値を発生させる初期値発生手段と、

前記初期値抽出手段により抽出した初期値と前記初期値発生手段で発生させた初期値の何れかを選択して出力する初期値選択手段と、

前記初期値選択手段で選択された初期値をもとにして第２の暗号を発生させる第２の暗号発生手段と、

前記第１の暗号発生手段から出力される第１の暗号と第２の暗号発生手段から出力される第２の暗号を選択して出力する暗号選択手段と、

前記暗号選択手段から出力される暗号をもとに、前記入力選択手段で選択した暗号化信号を復号する復号手段と、

前記第２の暗号発生手段で発生させた第２の暗号を用いて前記復号した信号を再暗号化する再暗号化手段と、

前記再暗号化手段で再暗号化した再暗号化信号に前記初期値発生手段で発生させた初期値を多重化する暗号初期値多重化手段と、

前記暗号初期値多重化手段から出力される信号を蓄積または伝送する蓄積伝送手段とを備え、

前記蓄積伝送手段に信号を蓄積または伝送する場合は、前記初期値選択手段の入力は前記初期値発生手段で発生させた初期値を選択し、前記暗号の選択手段は前記第１の暗号発生手段が出力する第１の暗号を選択し、

蓄積伝送手段から信号を再生する場合は、蓄積伝送手段から再生された信号は前記２つの暗号化信号入力手段にの何れかに入力し、前記入力選択手段は前記蓄積伝送手段からの入力を選択し、前記初期値選択手段は前記初期値抽出手段により抽出した初期値を選択し、前記暗号選択手段は第２の暗号発生手段が出力する第２の暗号を選択して出力することを特徴とする信号処理装置。

【請求項７】暗号化された信号を入力する暗号化信号入力手段と、

前記暗号化信号入力手段に入力した暗号化信号の中から初期値を抽出する初期値抽出手段と、

前記初期値抽出手段で抽出した初期値をもとにして第１の暗号を発生させる第１の暗号発生手段と、

前記第１の暗号発生手段で発生させた第１の暗号をもとにして前記暗号化信号入力手段に入力された暗号化信号を復号する復号手段と、

前記復号手段で復号した信号を所定長のブロックデータに分割するデータ分割手段と、

前記データ分割手段により所定長のブロックに分割したデータをそのブロック内で所定の順番に並べ替える第１

のデータ並べ替え手段と、
前記第１のデータ並べ替え手段で並べ替えたデータに対し同期データを付加して出力する同期付加手段と、
前記同期付加手段の出力データを蓄積または伝送する蓄積伝送手段と、
前記蓄積伝送手段から再生されたデータの中から同期データを検出して同期信号を出力する同期検出手段と、
前記同期検出手段から出力される同期信号をもとにして前記蓄積伝送手段から再生されたデータの中からブロック毎にデータを抽出するデータ抽出手段と、
前記データ抽出手段で抽出したデータをブロック内で所定の順番に並べ替え出力する第２のデータ並べ替え手段と、
前記復号手段から出力される復号信号と前記第２のデータ並べ替え手段から出力される信号の何れかを選択して出力する信号選択手段とを備え、
前記蓄積伝送手段に信号を伝送または蓄積する場合は、前記信号選択手段は前記復号手段から出力される復号信号を選択して出力し、前記蓄積伝送手段から信号を再生する場合は、前記信号選択手段は前記第２のデータ並べ替え手段から出力される信号を選択して出力することを特徴とする信号処理装置。
【請求項８】請求項７において、前記第２のデータ並べ替え手段の一部または全体を着脱可能としたことを特徴とする信号処理装置。
【発明の詳細な説明】
【０００１】
【産業上の利用分野】本発明は、暗号化された信号を復号する信号処理装置に関し、特に復号された信号の著作権を保護しつつ該復号信号の蓄積や伝送を可能とし、暗号化信号の復号及び蓄積または伝送に対して課金するのに適した信号処理装置に関する。
【０００２】
【従来の技術】衛星通信サービスにおける映像信号や音声信号の暗号化及び復号，課金システムに関する技術は、例えば、テレビジョン学会誌 Vol.46、No.1、pp31～39（１９９２年１月）に記載されている。
【０００３】
【発明が解決しようとする課題】情報圧縮技術を利用した多チャンネル有料デジタル放送では、その多数のチャンネルを利用して、同じ番組を複数のチャンネルで一定時間毎に時間をずらして放送するタイムシフト放送や、受信端末のリクエストに応じて番組を放送するビデオオンデマンドなどの新サービスを行なうことができる。また、信号自身をデジタルで送受信できるようにして劣化がなく高品質の情報を得ることができる。
【０００４】しかしながら、劣化がなく複製の容易な高品質のデジタル情報を得られるようになって大量の複製が行われるようになると、海賊版が横行し、著作権が侵害されて正常な有料放送の運営が阻害される可能性がある。従って、著作権を保護し、有料放送を正常に運営するためには、放送局は、送出する情報にスクランブルをかけて該情報を保護する必要がある。

【０００５】しかしながら、受信装置でスクランブルを解いて復号した情報は、保護（スクランブル）が解除された形態であるので、この復号情報を蓄積したり伝送したりすると保護が継続しなくなってしまう問題がある。
【０００６】本発明の目的は、暗号化された信号を復号する信号処理装置に関し、特に復号された信号の著作権を保護しつつ該信号の蓄積及び伝送を可能とし、該信号の復号及び蓄積または伝送に対し課金するのに適した信号処理装置を提供することにある。
【０００７】
【課題を解決するための手段】前記目的を達成するために、本発明は、暗号化された入力信号の中から暗号の初期値を抽出する初期値抽出手段と、前記初期値をもとに第１の暗号を発生させる第１の暗号発生手段と、前記暗号化された入力信号を前記第１の暗号を使用して復号する復号手段とを備えた信号処理装置において、前記初期値抽出手段で抽出した初期値をもとにして新たな初期値を発生させる初期値発生手段と、前記初期値発生手段で発生させた新たな初期値をもとにして第２の暗号を発生させる第２の暗号発生手段と、前記第２の暗号発生手段で発生させた第２の暗号を用いて前記復号した入力信号を再暗号化する再暗号化手段と、前記再暗号化手段で再暗号化した信号に前記新たな初期値を多重化して外部装置や蓄積装置に対して出力する暗号の初期値多重化手段とを設けたことにある。
【０００８】また、外部装置や蓄積装置に伝送蓄積した信号を再生するために、複数の暗号化信号を入力する暗号化信号入力手段と、入力した複数の暗号化信号を選択する入力選択手段と、選択された暗号化信号の中から暗号の初期値を抽出する初期値抽出手段と、前記初期値抽出手段により抽出された初期値をもとに新たな初期値を発生する初期値発生手段と、選択された暗号化信号に対応した複数の暗号を発生する暗号発生手段と、前記暗号発生手段で発生した複数の暗号の何れかを選択する暗号選択手段と、選択した暗号をもとに暗号化信号を復号する復号手段とを設けたことを特徴とする。
【０００９】また、暗号化された入力信号の中から暗号の初期値を抽出する初期値抽出手段と、抽出された前記初期値をもとに第１の暗号を発生させる第１の暗号発生手段と、第１の暗号発生手段で発生させた第１の暗号をもとに前記暗号化された入力信号を復号する復号手段と、復号手段により復号した信号を所定長のブロックデータに分割するデータ分割手段と、データ分割手段により所定長のブロックに分割したデータをそのブロック内で所定の順番に並べ替える第１のデータ並べ替え手段と、第１のデータ並べ替え手段で並べ替えたデータに対し同期データを付加して出力する同期付加手段と、同期

付加手段の出力データを蓄積または伝送する蓄積伝送手段と、蓄積伝送手段から再生されたデータの中から同期データを検出する同期検出手段と、同期検出手段から出力される同期信号をもとにして前記蓄積伝送手段から再生されたデータの中からブロック毎にデータを抽出するデータ抽出手段と、データ抽出手段で抽出したデータをブロック内で所定の順番に並べ替えて出力する第２のデータ並べ替え手段と、前記復号手段から出力される復号信号と前記第２のデータ並べ替え手段から出力される信号の何れかを選択して出力する信号選択手段とを設けたことを特徴とする。

【００１０】

【作用】初期値抽出手段は暗号化された入力信号の中から暗号の初期値を抽出し、第１の暗号発生手段はこの初期値をもとにして第１の暗号を発生し、復号手段は第１の暗号をもとに前記暗号化された入力信号を復号する。

【００１１】初期値発生手段は、初期値抽出手段で抽出した初期値をもとにして新たな初期値を発生し、第２の暗号発生手段は前記新たな初期値をもとにして第２の暗号を発生する。暗号化手段は、前記第２の暗号を用いて前記復号信号を暗号化し、更に、初期値多重化手段により新たな初期値を多重化して出力する。

【００１２】これにより、復号した信号を別の暗号で再暗号化して、装置外部または蓄積装置に対して出力することができ、復号された信号の著作権を保護しつつ該信号の復号や蓄積，伝送に対し課金することができる信号処理装置が得られる。

【００１３】また、入力選択手段は暗号化信号入力手段により入力した複数の暗号化信号を選択し、初期値抽出手段は、選択された暗号化信号に含まれる暗号の初期値を抽出する。初期値発生手段は、抽出された初期値をもとにして新たな初期値を発生する。暗号発生手段は、この新たな初期値をもとにして複数の暗号を発生する。暗号選択手段は、選択された暗号化信号に対応した暗号を選択し、復号手段は、入力した暗号化信号をこの暗号をもとにして復号し、形式変換後に出力する。

【００１４】これにより、外部装置や蓄積装置からの複数の再生信号を暗号化信号入力手段に入力することで、それぞれの暗号で暗号化された信号を復号することが可能な信号処理装置を得ることができる。

【００１５】また、初期値抽出手段は、暗号化信号入力手段により入力した暗号化信号から暗号の初期値を抽出する。第１の暗号発生手段は、この初期値をもとに第１の暗号を発生させ、復号手段はこの第１の暗号をもとにして暗号化信号を復号し出力する。

【００１６】データ分割手段は、復号手段により復号した信号を所定長のブロックデータに分割し、第１のデータ並べ替え手段は、所定長のブロックに分割されたデータをそのブロック内で所定の順番に並べ替え、同期付加手段は、第１のデータ並べ替え手段で並べ替えたデータに対して同期データを付加し、これを蓄積伝送手段に蓄積または伝送する。

【００１７】また、同期検出手段は、蓄積伝送手段から再生されたデータの中から同期データを検出して同期信号を出力する。データ抽出手段は、前記同期信号をもとに蓄積伝送手段から再生されたデータの中からブロック毎にデータを抽出し、第２のデータ並べ替え手段は、抽出したデータをブロック内で所定の順番に並べ替えて出力する。そして、信号選択手段は、復号手段から出力される復号信号と第２のデータ並べ替え手段の出力信号の何れかを選択し出力する。

【００１８】これにより、復号した信号のデータの順番を入れ替えることで暗号化して、装置外部または蓄積装置に対して出力することができ、復号された信号の著作権を保護しつつ該信号の復号や蓄積または伝送に対して課金することができる信号処理装置を得ることができる。

【００１９】

【実施例】本発明の一実施例を図１を参照して説明する。図１は、本発明になる信号処理装置を受信端末に適用した通信衛星を利用した多チャンネル有料デジタル放送のシステムを示すブロック図である。

【００２０】図１において、１００は通信衛星を利用した多チャンネル有料デジタル放送を行なう放送局、２００は通信衛星、３００は金融機関、４００は多チャンネル有料デジタル放送を受信する受信端末、５００は前記放送局１００，金融機関３００，受信端末４００を互いに結んで双方向で通信可能な例えば電話回線等の低伝送レートの通信回線、６００は地上の放送局１００と通信衛星２００を結ぶ通信回線、７００は通信衛星２００と受信端末４００を結ぶ通信回線である。

【００２１】先ず、本発明になる受信端末を含む通信衛星を利用した多チャンネル有料デジタル放送システム及びその課金方法について説明する。

【００２２】多チャンネル有料デジタル放送のサービスを受けようとする加入者は、郵便や受信端末４００から通信回線５００を介して、放送局１００に対して加入申込を行ない、提携している金融機関３００に対して加入料金を振り込む。放送局１００は、これを確認すると、加入者に対してＩＤを割当て、例えば、ＩＣカードを送付することで受信端末４００を認証する。加入者はこれに対応した受信端末４００を開設し、サービスを受けることができるようにする。放送局１００は、著作権を保護するために送出する放送データにスクランブルをかけて送出する。

【００２３】通信回線６００を介してこの放送データを受けた通信衛星２００は、上り回線から下り回線への搬送周波数の変換等の処理を行い、通信回線７００を介して所定のサービスエリアに対して放送する。

【００２４】通信衛星２００の放送電波を受信した受信

端末４００は、放送局１００から配送されたＩＣカード等を用いてスクランブルを解除し、放送データを視聴することができるようにする。

【００２５】放送局１００は、通信回線５００を介して受信端末４００における番組視聴状況を調べ、例えば、契約月毎，契約チャンネル毎，視聴した放送番組毎等のさまざまな形態で課金し、金融機関３００を介して視聴料金を集金するようにする。

【００２６】次に、通信衛星を利用した多チャンネル有料デジタル放送を行う放送システムにおける放送局１００のについて説明する。図２は、前記放送局１００の内部構成を示すブロック図である。

【００２７】図２において、１０１は例えばＶＴＲやＤＡＴ，光磁気ディスク装置，光ディスク装置，ハードディスク装置，半導体メモリ装置等から放送データの再生を行う再生装置、１０２は再生された映像や音声等の情報の圧縮を行う圧縮装置、１０３は圧縮された情報信号を時分割で多重する多重化装置、１０４は暗号の初期値の発生や送出する放送データの管理及び顧客管理を一括して行う情報管理装置、１０５は暗号発生装置、１０６は暗号化装置、１０７は暗号の初期値や個別情報等と圧縮信号を多重化する多重化装置、１０８は通信衛星に対して放送データを送出するための変調等の処理を行う送出装置、１０９は顧客情報を管理する顧客情報データベース、１１０は受信端末４００からのリクエストや加入申込，課金のための視聴状況の確認等を行うための低伝送レートの双方向通信回線５００との接続端子、１１１は通信衛星２００に対して圧縮多重化した放送データを送出するための出力端子である。

【００２８】通信衛星を利用した多チャンネル有料デジタル放送では様々な新サービスが可能であるが、ここでは新サービスの一例としてビデオオンデマンドを例に挙げて放送局１００の内部の構成について説明する。

【００２９】通信回線５００及び接続端子１１０を介して受信端末４００からのリクエストを受け付けた場合は、情報管理装置１０４は、顧客情報データベース１０９を検索して、正規加入者か否かと視聴料金の支払状況の確認を行い、放送データの提供に適合する受信端末４００の場合には、再生装置１０１を用いてリクエストされた放送データを放送する。再生装置１０１で再生した放送データは、圧縮装置１０２で、例えば映像や音声であればＭＰＥＧ（Moving Picture Experts Group）方式などのような情報の特性に合わせた最適な圧縮方法で圧縮し、多重化装置１０３で他の圧縮された番組と共に時分割で多重化される。

【００３０】また、情報管理装置１０４は暗号を発生させるための暗号の初期値を管理し、暗号の初期値を発行し、暗号発生装置１０５及び多重化装置１０７に与える。

【００３１】暗号発生装置１０５は、情報管理装置１０４から受け取った暗号の初期値をもとにして、例えば疑似乱数などの暗号を発生させる。暗号化装置１０６は、この暗号をもとに、例えば、圧縮多重化した情報信号と暗号の排他的論理和を取つて暗号化する。更に、多重化装置１０７では、該暗号の初期値や個別情報及び番組情報等と圧縮信号を多重化する。ここでは説明を省略したが、多重化装置１０７で多重化する暗号の初期値や個別情報，番組情報等も暗号化することで、顧客のプライバシーの保護や暗号の不正な解読の防止することができ、システムの安全性を一段と向上させることもできる。

【００３２】そして、送出装置１０８によりエラー訂正符号の付加やデータのパケット化の他に通信衛星２００へ伝送するための変調処理を行い、出力端子１１１及び通信回線６００を介して通信衛星２００へ暗号化信号を伝送する。

【００３３】次に、図３は、前記受信端末４００の内部構成を示すブロック図である。４０１は通信衛星から放送された暗号化信号を入力する受信信号入力端子、４０２は受信した暗号化信号の復調，エラー訂正等を行う受信装置、４０３は該受信端末４００の全体を制御する制御装置、４０４は受信装置４０２の出力信号と蓄積装置であるハードディスク装置４１３の再生信号を切り替える入力信号選択装置、４０５は入力信号選択装置４０４で選択された暗号化信号の中から暗号の初期値を抽出する初期値分離装置、４０６は第１の暗号発生装置、４０７は第２の暗号発生装置、４０８は前記第１の暗号発生装置４０６から出力される暗号と第２の暗号発生装置４０７から出力される暗号を切り替えて選択する暗号選択装置、４０９は復号装置、４１０は再生装置、４１１は暗号化装置、４１２は暗号化装置４１１で暗号化した信号に暗号の初期値を多重する多重化装置、４１３は例えばハードディスク装置などの蓄積装置、４１４は該受信端末４００と通信回線５００を接続する通信回線接続端子、４１５は初期値発生装置、４１６は初期値選択装置である。

【００３４】デジタル信号を蓄積する蓄積装置４１３としては、デジタルＶＴＲ，ＤＡＴ，光磁気ディスク装置，半導体メモリ装置などがあるが、ここではハードディスク装置を例にとって説明する。また、蓄積する情報は、映像や静止画あるいは音声だけでなくアプリケーションソフトウェアや各種データの場合もあるので、この蓄積装置４１３は、ランダムアクセスの可能な装置であることが望ましい。

【００３５】図３では図示を省略しているが、通信衛星２００からの電波を受信するには、例えば室内や屋外に設置したパラボラアンテナ等のアンテナが必要であり、アンテナで受信した放送受信信号は、受信信号入力端子４０１を介して受信装置４０２に入力される。受信装置４０２は、復調の他に降雨落雷などによる通信回線７００の通信障害によるデータの欠落や誤りを訂正，補完し

て出力する。

【００３６】放送信号を受信する場合には、制御装置４０３は、入力信号選択装置４０４が受信装置４０２からの入力信号を選択するようコマンドを発行する。入力信号選択装置４０４は、制御装置４０３からのコマンドに従って入力系を切り替えて受信装置４０２からの入力信号を出力する。

【００３７】初期値分離装置４０５は、入力信号選択装置４０４から出力される信号の中から暗号の初期値や個別情報及び番組情報等を抽出する。これらの情報が暗号化されている場合には復号して出力する。この初期値分離装置４０５で抽出した暗号の初期値は、第１の暗号発生装置４０６に入力する。

【００３８】第１の暗号発生装置４０６は、この初期値を用いて暗号を発生する。第１の暗号発生装置４０６は、放送局１００内の暗号発生装置１０５と同じアルゴリズムで暗号を発生させる暗号発生装置とする。更に、第１の暗号発生装置４０６の一部またはは全体を、例えば、ＩＣカードに内蔵し、該受信端末４００から着脱可能な構造にしておけば、該ＩＣカードを加入者に配送することで、放送局１００内の暗号発生装置１０５と第１の暗号発生装置４０６のアルゴリズムを定期的に変更することが可能になり、不正視聴防止効果を一層高めることができる。この第１の暗号発生装置４０６から出力された暗号は、暗号選択装置４０８に入力する。

【００３９】暗号選択装置４０８は、制御装置４０３からのコマンドに従い、入力系を切り替える。つまり、通信衛星２００からの放送信号を受信中である場合には、第１の暗号発生装置４０６から入力される暗号を選択して出力する。

【００４０】復号装置４０９は、暗号選択装置４０８から出力された暗号をもとに、受信した暗号化信号を復号する。放送局１００内の暗号化装置１０６で、例えば、圧縮多重化した放送データ信号と暗号の排他的論理和を取って暗号化した放送信号が送出されている場合には、受信した暗号化信号と暗号選択装置４０８から出力される暗号の排他的論理和を取ることで元の放送データ信号に復号することができる。更に、放送データ信号が時分割多重化されている場合は、制御装置４０３からのコマンドに従い、該制御装置４０３が指示するチャンネルを選択して出力する。

【００４１】図３では図示を省略しているが、再生装置４１０の入力には、例えばＭＰＥＧデコーダ等の各種デコーダがあり、復号装置４０９で復号された放送データ信号がＭＰＥＧ方式で圧縮された信号の場合にはＭＰＥＧデコーダで伸長し、再生装置４１０のＤ／Ａ変換や走査線変換等の特性に合わせた形式変換を行なって該再生装置４１０で再生する。再生装置４１０は、例えば、伸長された信号が映像や静止画，アプリケーションソフトウェア，各種データの場合は、ＴＶモニタやコンピュータモニタ，ビデオプリンタ，プリンタ，ファクシミリ，コピー機であり、音声の場合はスピーカである。

【００４２】一方、受信した放送データ信号をハードディスク装置４１３に蓄積しようとする場合は、初期値分離装置４０５で抽出した暗号の初期値を初期値発生装置４１５に入力する。この初期値発生装置４１５は、初期値分離装置４０５から出力される初期値をもとにして新たに初期値を発生させて出力する。例えば、初期値分離装置４０５の内部には、初期値の変換テーブルを内蔵し、入力された初期値に応じて変換した新たな初期値を出力する。初期値を変換することで、受信端末４００が信号蓄積時の新たな初期値を管理することができるようになり、暗号の秘守性を向上させることができる。また、初期値分離装置４０５が出力する初期値に依存しない新たな初期値を発生させることもでき、各受信端末４００が信号蓄積時の新たな初期値を独自に管理することができるようにする。また、初期値分離装置４０５が出力する初期値をそのまま出力する構成を採用すると、初期値発生装置４１５を省略することもできる。

【００４３】初期値発生装置４１５から出力した新たな初期値は、初期値多重化装置４１２及び初期値選択装置４１６に入力する。初期値選択装置４１６は、制御装置４０３からのコマンドに従い、入力系を切り替える。つまり、受信した放送データ信号をハードディスク装置４１３に蓄積しようとする場合は、初期値発生装置４１５からの入力をを選択して出力する。初期値選択装置４１６から出力した新たな初期値は、第２の暗号発生装置４０７に入力する。

【００４４】暗号化装置４１１は、復号装置４０９で復号して出力される放送データ信号を、初期値選択装置４１６から出力された初期値をもとに、第２の暗号発生装置４０７で発生させた暗号を用いて、再び暗号化して出力する。そして、初期値多重化装置４１２は、この再暗号化された放送データ信号を、初期値発生装置４１５で発生させた初期値と多重化する。

【００４５】また、図３では図示を省略しているが、ハードディスク装置４１３の入力系には、データを該ハードディスク装置４１３に蓄積するために、例えば、エラー訂正符号の付加，ディレクトリ構成情報の付加，ハードディスク装置４１３のセクタフォーマットに合わせたデータの分割などのように該データの形式を変換する装置があり、入力された信号のデータ形式を変換して該ハードディスク装置４１３に蓄積する。

【００４６】第２の暗号発生装置４０７は、ハードディスク装置４１３を内蔵または外付けする各受信端末４００毎に異なるアルゴリズムで暗号を発生する暗号発生装置とし、該第２の暗号発生装置４０７の一部または全体を、例えば、ＩＣカードに内蔵し、該受信端末４００に着脱可能な構造にしておけば、ハードディスク装置４１３を内蔵または外付けする各受信端末４００の第２の暗

号発生装置４０７を異なるアルゴリズムとすることが容易となる。その結果、蓄積した放送データ信号のみを他の受信端末４００へ複写または移動しても第２の暗号発生装置４０７のアルゴリズムが異なる別の受信端末４００では再生できず、蓄積した放送データの著作権を保護することができる。

【００４７】しかし、ＩＣカードを合わせて移動することで、他の受信端末４００でも再生することができるようになり、第２の暗号発生装置４０７をＩＣカード化した場合の加入者の利便性を確保することができる。

【００４８】ハードディスク装置４１３に蓄積されている情報を再生する場合は、制御装置４０３は、入力信号選択装置４０４に対してハードディスク装置４１３からの入力信号を選択させるコマンドを発行する。入力信号選択装置４０４は、制御装置４０３からの前記コマンドに従って入力系を切り替え、ハードディスク装置４１３からの入力信号を選択して出力する。

【００４９】初期値分離装置４０５は、入力信号選択装置４０４からの出力信号の中から、暗号の初期値や個別情報，番組情報等を抽出する。これらの情報が暗号化されている場合には復号して出力する。初期値分離装置４０５で抽出された暗号の初期値は、初期値選択装置４１６に入力される。初期値選択装置４１６は、制御装置４０３からのコマンドに従って入力系を切り替える。つまり、ハードディスク装置４１３に蓄積されている情報を再生する場合は、初期値分離装置４０５からの入力信号を選択して出力する。初期値選択装置４１６で選択した初期値は、第２の暗号発生装置４０７に入力される。

【００５０】第２の暗号発生装置４０７は、初期値選択装置４１６で選択して入力される初期値を用いて暗号を発生して暗号選択装置４０８に入力する。暗号選択装置４０８は、入力信号選択装置４０４と同様に、制御装置４０３からのコマンドに従って入力系を切り替える。つまり、ハードディスク装置４１３に蓄積されている情報を再生する場合は、第２の暗号発生装置４０７から入力される暗号を選択して出力する。復号装置４０９は、暗号選択装置４０８から入力した暗号をもとに、ハードディスク装置４１３から再生される信号を復号する。この復号信号は、再生装置４１０で再生される。

【００５１】復号装置４０９から出力される復号信号は、情報の劣化や欠落がない高品質のディジタル信号であり、この復号信号をそのままの形で蓄積装置に蓄積できるようにすると、複製が可能となって著作権の保護が困難になる。しかし、以上に説明したように、特殊な条件化でしか復号できないように暗号化して蓄積装置に蓄積する構成とすることで、著作権を保護しかつ高品質の情報を蓄積したり、視聴することができるようになる。

【００５２】不正な複製による視聴を防止するため、放送局１００内の暗号発生装置１０５と第１の暗号発生装置４０６のアルゴリズムは定期的に変更される。従って、受信した暗号化信号をそのまま蓄積装置に蓄積しておくと、第１の暗号発生装置４０６のアルゴリズムが変更された場合は、それ以前に蓄積した暗号化信号を再生することができなくなる。そこで、受信した暗号化信号を蓄積するときには、受信した暗号化信号を復号した後に第２の暗号発生装置４０７からの暗号で再び暗号化して蓄積するようにすることで、以前に蓄積した暗号化信号も再生することができるようになる。

【００５３】そして、受信端末４００の内部またはＩＣカードの内部に、例えば、フラッシュメモリ等を用いたレジスタや記憶装置を設け、復号及び暗号化した回数や時間を記憶させ、放送局１００がこれを定期的に通信回線５００と制御装置４０３を介して調べることにより、受信端末４００またはＩＣカードに対してその利用状況に応じて課金することができる。受信端末４００の内部またはＩＣカードの内部の何れにレジスタや記憶装置を設けるかは、受信端末４００とＩＣカードの何れに対して課金するシステムにするかという選択肢と加入者の利用方法に応じて選択することも可能である。

【００５４】この実施例では、通信回線として通信衛星を例にあげたが、その他の通信回線、例えば、光ファイバーや同軸ケーブルを用いたケーブルテレビの通信回線、ＩＳＤＮ（Integrated Service Digital Network）等の電話回線なども使用可能である。また、第１の暗号発生装置４０６のアルゴリズムを定期的に変更する手段として、ＩＣカードを加入者に配送する方法を例示したが、通信回線５００及び通信回線接続端子４１４を介して第１の暗号発生装置４０６のアルゴリズムを変更するようにすることも可能である。

【００５５】次に、受信端末４００の変形例を図４を参照して説明する。

【００５６】図４において、４０１は通信衛星からの暗号化された放送信号を入力する受信信号入力端子、４０２は受信した放送信号の復調やエラー訂正等を行う受信装置、４０３は受信端末４００の全体を制御する制御装置、４０５は受信装置から出力される受信信号の中から暗号の初期値を抽出する初期値分離装置、４０６は第１の暗号発生装置、４０９は復号装置、４１０は再生装置、４１３は例えばハードディスク装置などの蓄積装置、４１４はこの受信端末４００と通信回線５００を接続する通信回線接続端子、４５０はデータブロック化装置、４５１は第１のデータ並べ替え装置、４５２は同期付加装置、４５３は同期検出装置、４５４はデータ抽出装置、４５５は第２のデータ並べ替え装置、４５６は信号選択装置である。

【００５７】図３に示した実施例と同様に、図４では図示を省略しているが、通信衛星２００からの電波を受信するには、例えば室内や屋外に設置したパラボラアンテナ等のアンテナが必要であり、アンテナで受信した放送信号を受信信号入力端子４０１を介して受信装置４０２

に入力する。受信装置４０２は、復調の他に降雨落雷などに起因する通信回線７００の通信障害によるデータの欠落や誤りを訂正補完して出力する。

【００５８】初期値分離装置４０５は、受信装置４０２からの出力信号の中から暗号の初期値や個別情報，番組情報等を抽出する。これらの情報が暗号化されている場合には復号して出力する。初期値分離装置４０５で抽出した暗号の初期値は、第１の暗号発生装置４０６に入力する。

【００５９】第１の暗号発生装置４０６はこの初期値を用いて暗号を発生する。この第１の暗号発生装置４０６は、放送局１００内の暗号発生装置１０５と同じアルゴリズムで暗号を発生させる暗号発生装置とする。更に、この第１の暗号発生装置４０６の一部または全体を、例えば、ＩＣカードに内蔵し、受信端末４００から着脱可能な構造にしておけば、ＩＣカードを加入者に配送することで放送局１００内の暗号発生装置１０５と第１の暗号発生装置４０６のアルゴリズムを定期的に変更することが可能になり、不正視聴を防止する効果を更に高めることができるようになる。

【００６０】第１の暗号発生装置４０６から出力された暗号は復号装置４０９に入力し、該復号装置４０９は受信した放送データ信号を該暗号を使用して復号する。放送局１００内の暗号化装置１０６で、例えば、圧縮多重化した信号と暗号の排他的論理和を取って暗号化して送出している場合には、受信した暗号化信号と第１の暗号発生装置４０６の出力する暗号の排他的論理和を取ることで元の情報信号に復号する。更に、信号が時分割多重化されている場合は、制御装置４０３からのコマンドに従って該制御装置４０３が指示するチャンネルを選択して出力する。

【００６１】復号した放送データは、信号選択装置４５６に入力する。制御装置４０３は、放送信号受信中は、信号選択装置４５６に対して復号装置４０９からの信号を選択するようにコマンドを発行する。信号選択装置４５６は、制御装置４０３からのコマンドに従って入力系を切り替える。

【００６２】図４では図示を省略しているが、再生装置４１０の入力系には、各種デコーダや形式変換装置があり、復号装置４０９で復号された放送データが、例えばＭＰＥＧ方式で圧縮されたデータの場合には、該データをＭＰＥＧデコーダで伸長し、再生装置４１０のＤ／Ａ変換や走査線変換等の特性に合わせた形式変換を行なってから該再生装置４１０で再生する。再生装置４１０は、例えば、伸長されたデータが映像や静止画，アプリケーションソフトウェア，各種データ等の場合は、ＴＶモニタやコンピュータモニタ，ビデオプリンタ，プリンタ，ファクシミリ，コピー機であり、音声の場合はスピーカである。

【００６３】次に、受信して復号した放送データをハードディスク装置４１３に蓄積しようとする場合は、復号装置４０９から出力される放送データをデータブロック化装置４５０に入力する。このデータブロック化装置４５０は、例えばバッファメモリを使用して構成され、復号装置４０９から出力される放送データを、一旦、バッファメモリに書き込んだ後に同期付加装置４５２から出力されるタイミング信号に合わせて読み出して出力することで、データを所定の長さのデータブロックに分割する。

【００６４】第１のデータ並べ替え装置４５１もデータブロック化装置４５０と同様に、例えばバッファメモリを使用して構成され、データブロック化装置４５０から出力されるブロック化したデータを、一旦、バッファメモリに書き込んだ後に同期付加装置４５２から出力されるタイミング信号に合わせて読み出すものである。書き込み時には連続した番地にデータを格納し、バッファメモリから読み出し時には、読み出す番地を所定の不連続順番とすることにより、ブロック内でのデータの並べ替えを行う。

【００６５】ここでは、データブロック化装置４５０のバッファメモリと第１のデータ並べ替え装置４５１のバッファメモリを別のものとして説明したが、これらの一連の処理を同一のバッファメモリを用いて処理することもできる。つまり、復号装置４０９が出力する復号データは、バッファメモリの連続した番地に書き込んだ後に同期付加装置４５２からのタイミング信号に合わせて読み出して出力することで、データを所定の長さのデータブロックに分割する。そして、読み出す番地を所定の順番で読み出すことにより、ブロック内でデータの並べ替えを行う。

【００６６】第１のデータ並べ替え装置４５１の出力データは、同期付加装置４５２に入力する。そして、同期付加装置４５２で同期データを付加して出力する。

【００６７】図５では図示を省略しているが、ハードディスク装置４１３に蓄積するためには、例えば、エラー訂正符号の付加，ディレクトリ構成情報の付加，ハードディスク装置４１３のセクタフォーマットに合わせたデータの分割などデータの形式変換が行われる。

【００６８】ハードディスク装置４１３から再生した暗号化信号は、エラー訂正等の処理を行った後に同期検出装置４５３へ入力する。同期検出装置４５３は、再生された信号の中から同期データを検出し、データ抽出装置４５４と第２のデータ並べ替え装置４５５にタイミング信号を与える。

【００６９】ハードディスク装置４１３から再生した暗号化信号は、データ抽出装置４５４へも入力する。データ抽出装置４５４と第２のデータ並べ替え装置４５５は、データブロック化装置４５０の第１のデータ並べ替え装置４５１と同様に同一のバッファメモリで構成することができる。つまり、ハードディスク装置４１３から

再生した信号はバッファメモリに書き込む。このとき、同期検出装置４５３から与えられるタイミング信号に合わせて、ハードディスク装置４１３から再生された信号中の同期データの部分の書き込みを禁止することで再生データのみを抽出する。書き込み時は、データを連続した番地に格納する。そして、同期検出装置４５３から出力されるタイミング信号に合わせてバッファメモリからデータを読み出して出力する。このとき、読み出す番地の順番を前記第１のデータ並べ替え装置４５１で並べ替えた順番と逆の順番とすることでデータをもとの順番に戻すことができる。

【００７０】第２のデータ並べ替え装置４５５の出力信号は、信号選択装置４５６に入力する。制御装置４０３は、再生中である場合には、信号選択装置４５６が第２のデータ並べ替え装置４５５からの入力信号を選択するようなコマンドを発行する。信号選択装置４５６は、制御装置４０３からのコマンドに従って入力系を切り替え、選択した信号を再生装置４１０に入力して再生する。

【００７１】第１のデータ並べ替え装置４５１及び第２のデータ並べ替え装置４５５は、各受信端末４００によって異なるのアルゴリズムとしておき、第２のデータ並べ替え装置４５５の一部または全体を、例えば、ＩＣカードに内蔵し、受信端末４００から着脱可能な構造にしておけば、例え、蓄積したデータを他の受信端末４００へ複写または移動しても第２のデータ並べ替え装置４５５のアルゴリズムが異なる多の受信端末４００では再生できず、蓄積したデータの著作権を保護することができる。データ抽出装置４５４と第２のデータ並べ替え装置４５５が同一のバッファメモリで構成されている場合には、バッファメモリの読み出し番地を発生させる部分を、例えば、ＩＣカードに内蔵するようにする。

【００７２】一方、蓄積したデータを他の受信端末４００へ複写または移動したときには、第２のデータ並べ替え装置４５５の一部または全体を内蔵したＩＣカードを合わせて移動することで、該他の受信端末４００でも該データを再生することができるようになり、加入者の利便性を確保することができる。

【００７３】そして、不正な視聴を防止するために放送局１００内の暗号化装置１０５と復号装置４０９のアルゴリズムを定期的に変更した場合でも、受信した暗号化信号を復号した後に第１のデータ並べ替え装置４５１でデータの順番を並べ換えて蓄積することで、著作権を保護し且つ高品質の情報を蓄積することが可能となる。そして、再生時には第２のデータ並べ替え装置４５５で並べ戻すことで、アルゴリズム変更前に蓄積した信号も再生することができるようになる。

【００７４】上記の実施例では、復号したデータを蓄積装置であるハードディスク装置４１３に蓄積する構成を例示したが、蓄積装置だけでなく、伝送装置を内蔵する構成も可能である。伝送装置として、例えば、モデムやＲＳ－２３２Ｃインターフェイス，ＳＣＳＩ（Small Computer System Interface）を内蔵し、復号したデータをこれらの伝送装置を用いて、例えば、コンピュータのメモリ上に転送したり、プリンタなどに出力するようにすることも可能である。

【００７５】次に、本発明の他の実施例を図５を参照して説明する。図５に示す実施例は、光ファイバーを用いたデジタルＣＡＴＶ（CAble TeleVision ケーブルテレビ）システムである。

【００７６】図５において、１００は図１及び図２に示した放送局とほぼ同じ機能をもつデジタルＣＡＴＶの放送局、１１０は受信端末４００からのリクエストや加入申込，課金のための視聴状況の確認，課金情報の伝送等を行うための通信回線８００との接続端子、１１１は中継局に対して圧縮多重化した番組放送データを送出するための出力端子、４００は図１及び図３に示した受信端末とほぼ同じ構成のデジタルＣＡＴＶの受信端末、４０１は中継局９００からの放送信号を入力する受信信号入力端子、４１４は受信端末４００からのリクエストや加入申込，課金のための視聴状況の確認，課金情報伝送等を行うための通信回線８０１との接続端子、８００は放送局１００と中継局９００を結ぶ通信回線、８０１は中継局９００と受信端末４００を結ぶ通信回線、９００は中継局、９０１は放送局１００からの放送信号を入力する受信信号入力端子、９０２は受信端末４００からのリクエストや加入申込，課金のための視聴状況の確認，課金情報の伝送等を行うための通信回線８００との接続端子、９０３は受信した放送信号の復調やエラー訂正等を行う受信装置、９０４は入力された放送受信信号の中から暗号の初期値を抽出する初期値分離装置、９０５は第１の暗号発生装置、９０６は復号装置、９０７は初期値発生装置、９０８は第２の暗号発生装置、９０９は暗号化装置、９１０は複数の受信端末４００に対し放送信号を分配する分配装置、９１１は中継局９００の全体を制御する制御装置、９１２は受信端末４００と中継局９００を結ぶ通信回線８０１との接続端子である。

【００７７】図１に示した実施例では、番組放送データを伝送する通信回線６００及び７００と、リクエストや加入申込，課金のための視聴状況の確認等を行うための通信回線５００は別の回線を使用しているが、図５に示した実施例である光ファイバーを用いたデジタルＣＡＴＶシステムでは、同一の通信回線８００，８０１を用いることができる。また、図５では図示を省略してあるが、１つの放送局１００からの放送信号を複数の中継局９００で受け、該中継局９００が更に複数の受信端末４００に分配する構成をとっている。この実施例では、中継局９００としているが、系列の地方または地域放送局とすることができる。

【００７８】図１に示した実施例と同様に、放送局１０

０は複数の番組放送データを圧縮多重化し、暗号化して出力端子１１１から出力する。光ファイバーを用いた通信回線８００は、この放送データを複数の中継局９００に伝送する。通信回線８００と受信信号入力端子９０１を介して受信した暗号化された放送信号は、受信装置９０３に入力する。受信装置９０３は、通信回線８００における通信障害によるデータの欠落や誤りを訂正補完して出力する。

【００７９】初期値分離装置９０４は、受信装置９０３から入力した受信信号の中から暗号の初期値を抽出する。初期値に関する情報が暗号化されている場合には復号する。初期値分離装置９０４で抽出した暗号の初期値は、第１の暗号発生装置９０５及び初期値発生装置９０７を介して第２の暗号発生装置９０８にそれぞれ入力し、それぞれで暗号を発生する。第１の暗号発生装置９０５は、放送局１００内の暗号発生装置１０５と同じアルゴリズムで暗号を発生させる暗号発生装置とする。

【００８０】復号装置９０６は、第１の暗号発生装置９０５から出力される暗号を用いて、受信した暗号化信号を復号する。

【００８１】初期値発生装置９０７は、初期値分離装置９０４から出力される初期値をもとに新たに初期値を発生する。この初期値発生装置９０７から出力される新たな初期値は第２の暗号発生装置９０８に入力し、この第２の暗号発生装置９０８はこの初期値をもとに暗号を発生する。また、この初期値発生装置９０７は、初期値分離装置９０４が出力する初期値をそのまま出力する構成を採用すると、初期値発生装置９０４を省略することもできる。更に、初期値分離装置９０４が出力する初期値に依存しない初期値を発生させて出力することもできる。初期値分離装置９０４を制御装置９１１で制御することにより、受信端末４００へ配信する暗号化信号の暗号を中継局９００が独自で管理することができるようになる。

【００８２】暗号化装置９０９は、第２の暗号発生装置９０８で発生した暗号を用いて復号装置９０６から出力される復号信号を再暗号化して出力する。分配装置９１０は、暗号化装置９０９からの入力信号を複数の受信端末４００に分配するために暗号化装置９０９からの入力信号を複数の接続端子９１２へ分配して出力する。

【００８３】そして、各受信端末４００は、接続端子９１２から通信回線８０１及び受信信号入力端子４０１を介して出力信号を受信する。通信回線８０１は双方向であり、放送局１００へのリクエストや加入申込，課金のための視聴状況の確認，課金情報の伝送等の情報交換は、接続端子４１４，通信回線８０１，分配装置９１０を介した制御装置９１１と受信端末４００の間の通信で行なう。更に、中継局９００と放送局１００の間の通信は、制御装置９１１から接続端子９０２，通信回線８００，接続端子１１０を介して行なう

図５では図示を省略したが、放送局１００についても放送する信号の暗号化のために中継局９００と同様の構成を採用することで、番組放送データ配給会社から暗号化されて送信されてきた番組放送データを復号し、該放送局１００が管理する独自の暗号の初期値と暗号で暗号化して中継局９００へ配信することが可能である。

【００８４】

【発明の効果】本発明は、復号した放送データ信号を再び別のアルゴリズムで暗号化して特定の条件化でしか復号できない形にして蓄積や伝送を可能としたので、放送データの著作権を保護し、且つ、信号がもつ情報品質を劣化させることなく、例えば、他の装置へ伝送したり、蓄積装置などに蓄積することがが可能となる。

【００８５】また、入力した暗号化信号の種類に応じて、それぞれの暗号発生装置で発生させた暗号をそれに応じて選択することで、それぞれのアルゴリズムで暗号化れた複数の信号を復号できる信号処理装置が得られる。

【００８６】更に、暗号発生手段や暗号化手段の一部または全体を着脱可能とすることにより、暗号発生や暗号化のアルゴリズムを容易に変更できるようになった。その結果、信号処理装置の不正な使用を防止したり、信号処理装置を個別に管理するこができるようになる。また、視聴に対し課金したり、放送データの著作権を保護したり、加入者の利便性を確保し、システム全体の安全性や使いがってを向上させることのできる信号処理装置が得られる。

【図面の簡単な説明】

【図１】本発明になる受信端末を含む通信衛星を利用した多チャンネル有料デジタル放送システムの全体構成を示すブロック図である。

【図２】図１に示した放送システムにおける放送局の内部構成を示すブロック図である。

【図３】図１に示した放送システムにおける受信端末の内部構成を示すブロック図である。

【図４】図１に示した放送システムにおける受信端末の内部構成の変形例を示すブロック図である。

【図５】本発明になる中継局を含む光ファイバーを用いたデジタルＣＡＴＶシステムの全体を示すブロック図である。

【符号の説明】

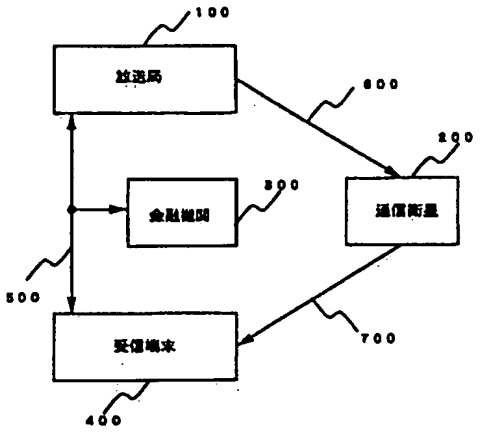
１００…放送局、１０１…再生装置、１０２…圧縮装置、１０４…情報管理装置、１０５…暗号発生装置、１０６…暗号化装置、２００…通信衛星、４００…受信端末、４０４…入力信号選択装置、４０５…初期値分離装置、４０６…第１の暗号発生装置、４０７…第２の暗号発生装置、４０８…暗号選択装置、４０９…復号装置、４１１…暗号化装置、４１３…蓄積装置、４１５…初期値発生装置、４５１…第１のデータ並べ替え装置、４５５…第２のデータ並べ替え装置、５００，６００，７０

19　　20

0，８００，８０１…通信回線、９００…中継局、９０４…初期値発生装置、９０５…第１の暗号発生装置、９０６…復号装置、９０８…第２の暗号発生装置、９０９…暗号化装置、９１０…分配装置。

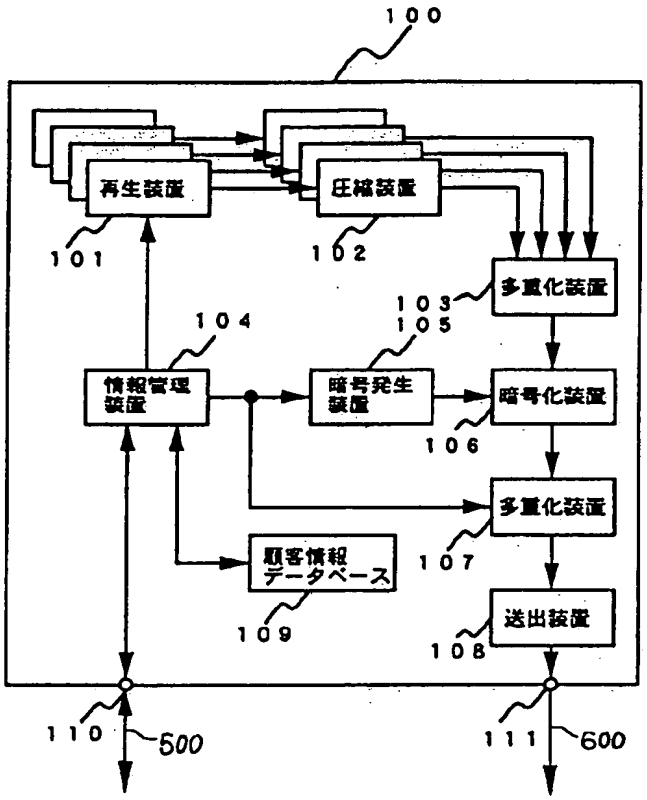
【図１】

図１



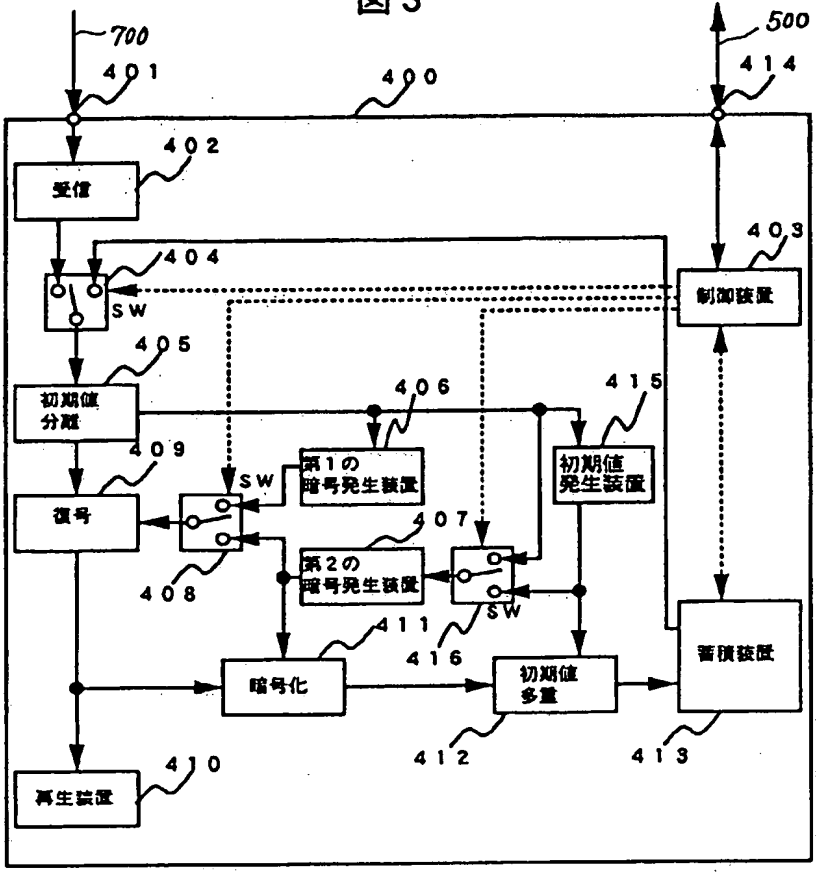
【図2】

図2


100
再生装置
101
圧縮装置
102
多重化装置
103
104
105
情報管理装置
暗号発生装置
暗号化装置
106
多重化装置
107
顧客情報データベース
109
送出装置
108
110
500
111
600

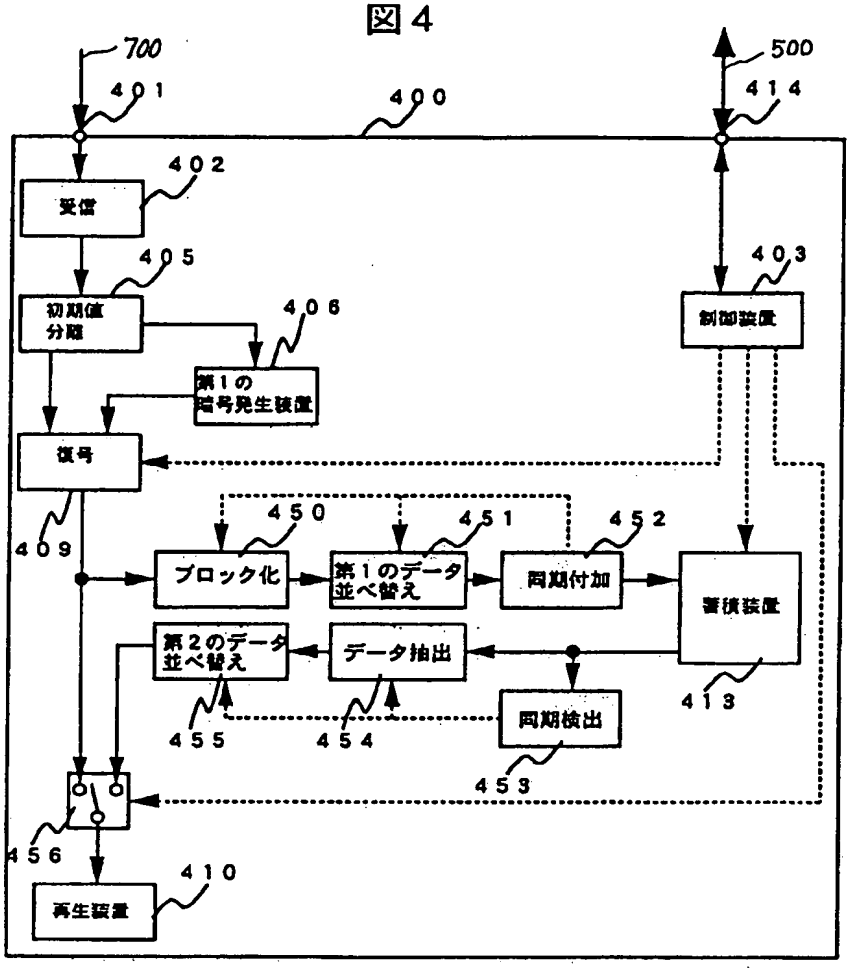
【図3】

図３


700
401
400
500
414
402
受信
403
制御装置
404
SW
405
初期値
分離
406
415
409
第1の
暗号発生装置
初期値
発生装置
SW
復号
407
第2の
暗号発生装置
408
SW
411
416
暗号化
初期値
多重
蓄積装置
412
413
410
再生装置

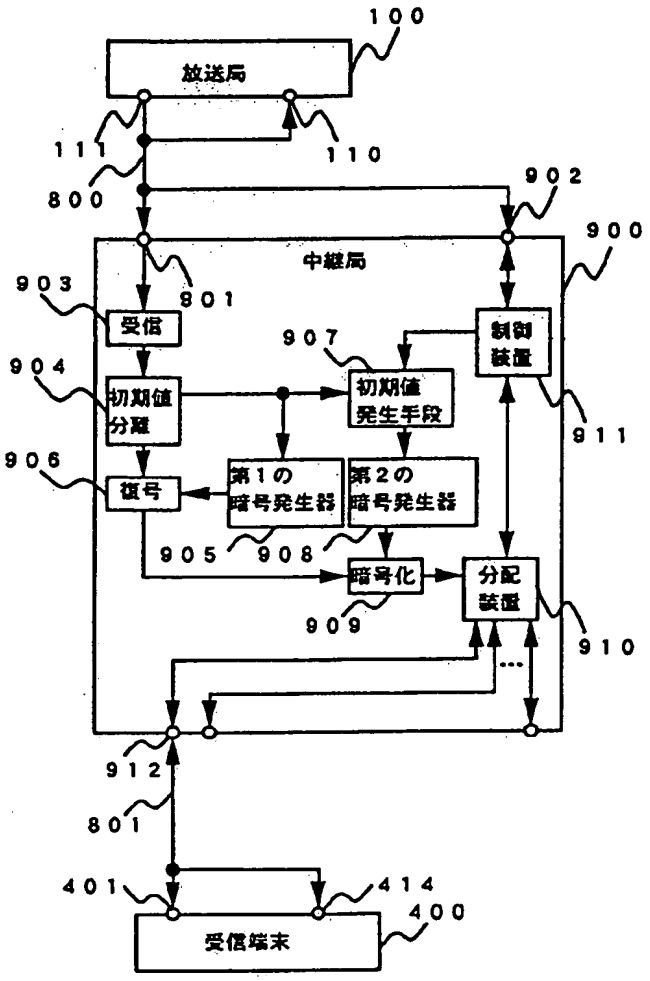
【図4】

図４


700
401
400
500
414
402
受信
405
初期値分離
406
第1の信号発生装置
403
制御装置
復号
409
450
451
452
ブロック化
第1のデータ並べ替え
同期付加
蓄積装置
413
第2のデータ並べ替え
データ抽出
455
454
同期検出
453
456
410
再生装置

【図5】

図5



フロントページの続き

(51)Int.Cl.6	識別記号	庁内整理番号	FI	技術表示箇所
H04H 1/00		H F		

(72)発明者　細川　恭一
神奈川県横浜市戸塚区吉田町292番地　株式会社日立製作所映像メディア研究所内

(72)発明者　杉村　直純
神奈川県横浜市戸塚区吉田町292番地　株式会社日立製作所映像メディア研究所内

(72)発明者　尾鷲　仁朗
神奈川県横浜市戸塚区吉田町292番地　株式会社日立製作所映像メディア研究所内

(72)発明者　橘　浩昭
神奈川県横浜市戸塚区吉田町292番地　株式会社日立製作所情報映像メディア事業部内